

IN THE CLAIMS

Please amend Claims 1, 5-10, and 14 as follows. The following is a complete listing of the claims in the present application, reflects all changes which have been made to the claims, and replaces all earlier versions and all earlier listings of the claims:

1. (Currently Amended) A method for facilitating changes to security systems, said method including:

detecting a back-end security update in a back-end database;

~~detecting non-conforming information between comparing said back-end security update to database and a front-end database storing front-end security information stored on a front-end database; [[and]]~~

~~generating an update command for reconstructing said back-end database to conform to said front-end database and storing said update command in at least one of said back-end database and said front-end database; and~~

~~executing said update command.~~

2. (Original) The method according to claim 1, further comprising the step of filtering back-end database information.

3. (Original) The method according to claim 2, wherein said step of filtering back-end database information includes employing naming conventions.

4. (Original) The method according to claim 1, further comprising the step of transferring information from said back-end database to said front-end database.
5. (Currently Amended) The method according to claim 1, wherein said back-end security update is a Remote Access Control Facility (RACF) update.
6. (Currently Amended) The method according to claim 1, wherein said back-end security update is a Transaction Processing Facility (TPF) update.
7. (Currently Amended) The method according to claim 1, wherein said back-end security update is a Computer Associate's Access Control Facility 2 (CA-ACF2) update.
8. (Currently Amended) The method according to claim 1, wherein said back-end security update is a Lightweight Directory Access Protocol (LDAP) update.
9. (Currently Amended) The method according to claim 1, wherein said step of reconstructing generating the update command further includes at least one of the steps of:
 - matching information stored on a back-end database to information stored on a front-end database,
 - generating a counteracting command sequence,

transferring said command sequence from a front-end system to a back-end system, and

executing said command ~~system~~ sequence.

10. (Currently Amended) A security system including:

a device configured to detect a back-end security update on a back-end database;

a device configured to detect non-conforming information between ~~compare~~ said back-end security update to database and a front-end database storing front-end security information ~~stored on a front-end database~~; and

a device configured to generate and execute an update command for reconstructing ~~reconstruct~~ said back-end database to conform it to said front-end database.

11. (Original) The system according to claim 10, wherein said devices are configured to operate in one of a real time and batch processing mode.

12. (Original) The system of claim 10, wherein said front-end database includes two or more data tables.

13. (Original) The system of claim 10, wherein said device configured to detect said back-end security update is further configured to filter back-end update information.

14. (Currently Amended) A method for facilitating changes to security systems, said method including:

sending a back-end update from a local back-end system to a front-end database;

detecting said back-end update on said front-end database;

formatting said back-end security update to create an update command; [[and]]

transferring said update command to a remote back-end system; and

executing said update command to reconstruct said back-end database.

15. (Original) The method of claim 14, wherein said step of formatting includes assigning a destination to said update command.